APPLICATION UNDER UNITED STATES PATENT LAWS

Invention: **DEPLOYABLE SECURE COMMUNICATION SYSTEM**

Inventor(s): Steve ANSPACH;
Jose LLERAS;
Luke SALAZAR; and
Greg KASSON

Manelli Denison & Selter PLLC
2000 M Street, NW
7th Floor
Washington, DC 20036-3307
Attorneys
Telephone: (202) 261-1000

This is a:

[ ] Provisional Application

[X] Regular Utility Application

[ ] Continuing Application

[ ] PCT National Phase Application

[ ] Design Application

[ ] Reissue Application

[ ] Plant Application

SPECIFICATION

DEPLOYABLE SECURE COMMUNICATION SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to computer and communication networks, and more specifically, to a deployable communication system used to provide secure voice, video and data services to multiple remote users.

2. Background of Related Art

Conventional deployable communication systems exist:

- Turtle Mountain – TMC PCS-M4 - http://www.turtle-mtn.com/pcsm4.pdf
- General Dynamics –ReadySET- http://www.gd-decisionsystems.com/readyset/
- Raytheon – T-VSAT - http://www.raytheon.com/c3i/c3iproducts/c3i076/c3i076.htm
- AOS Inc - GCS Netlink GAN- http://www.aosusa.com/netlink_m4.html
- NERA WorldCommunicator - http://www.aosusa.com/neraworldcom.htm
- Global Communication Solutions Inc. - GCS 400 Series - http://www.globalcoms.com/Pages/custom_systems/gcs400_series.htm
- Mobile Telesystems Inc -MTI-M4-128 - http://mti-usa.com/
- LOGIX- Portable Satellite Communication Suitcase - http://www.logixusa.com/Products.html#immar

Fig. 9 is a depiction of a particular conventional deployable secure communication system.

In particular, as shown in Fig. 9, a secure encryption module such as defined by KIV-7 standards **912** with suitable interface hardware

is utilized in a direct connection path between a remote user **910** and a wireless connection to a similarly secure receiver via a satellite antenna **914**. In the conventional system of Fig. 9, an ISDN link is utilized between the module **912** including a KIV-7 encryption module, and a suitable satellite two-way communication transceiver and antenna **914**.

However, such conventional systems are typically physically large but more importantly allow for only direct connection communication between a remote user and a receiver to maintain security in the communications. While this is quite useful in many situations, only limited communications are possible in a direct connection. For instance, direct connectivity does not allow access to wired public communication systems, e.g., the Internet.

There is a need for a small, lightweight, easily portable and easily deployable communication system that permits broader functionality than that available using a direct connection, including direct access to a public network system.

BRIEF DESCRIPTION OF THE DRAWINGS

Features and advantages of the present invention will become apparent to those skilled in the art from the following description with reference to the drawings, in which:

Fig. 1 is a block diagram of an exemplary deployable secure communication system, in accordance with a first embodiment of the present invention.

Fig. 2 is a more detailed block diagram of the exemplary deployable secure communication system shown in Fig. 1.

Fig. 3 shows a graphic depiction of another exemplary deployable communication system in communication with a gateway network, in accordance with another aspect of the present invention.

Fig. 4 shows an exemplary network server module, in accordance with the principles of the present invention.

Fig. 5 shows an exemplary network WAN module, in accordance with the principles of the present invention.

Fig. 6 shows an exemplary network encryption module, in accordance with the principles of the present invention.

Fig. 7 shows a universal power module, in accordance with the principles of the present invention.

Fig. 8 shows a low profile deployable secure communication system integrating a network server module, a network WAN module, an encryption module, and a universal power module, in accordance with the principles of yet another aspect of the present invention.

Fig. 9 is a depiction of a particular conventional deployable secure communication system.

SUMMARY OF THE INVENTION

In accordance with the principles of the present invention, a method for providing network functionality and voice-over-IP services to a remote user at a deployed location comprises providing an encryption module having a secure side and a non-secure side. The non-secure side of the encryption module is accessed with bulk network data. The bulk network data is passed through the encryption module to produce encrypted bulk network data. The encrypted bulk network data is encapsulated in IP packets. The encapsulated encrypted bulk network data is routed through an Internet.

In accordance with another aspect of the invention, a method of providing a deployable communication system comprises passing network data through a KIV type encryption device to provide bulk encrypted data. The bulk encrypted data is encapsulated in IP packets. The IP encapsulated, bulk encrypted data is routed over an Internet. The

deployable communication system enables routing of secure communications via the Internet.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

The present invention provides secure Voice-Over-IP (VOIP), video and data network functionality in a single, small size deployable case, to a remote user. While capable of secure communications, the disclosed system also provides communication capability (VOIP, video and/or data) in a non-secure manner if desired. Most importantly, the present invention allows for the routing of bulk encrypted (i.e., secure) data over a public network, e.g., the Internet. The disclosed deployable system provides these capabilities without the need to remove and assemble components.

The disclosed deployable secure communications system can be deployed even at the most remote regions of the world where no other communication means are available, taking advantage of the satellite direct connection link, or (very importantly) in more developed regions that might include access to the Internet (e.g., in a hotel room, high speedx).

The disclosed deployable secure communications system can be deployed to provide a multitude of applications for remote users. Uses include emergency response, news reporting, public safety, drilling and mining operations, field surveys and other activities that require remote capabilities for video and data transmissions.

The system, once deployed and operational, offers access to the Internet or corporate network using a direct link via an Inmarsat M4 GAN network or ISDN terrestrial circuit. For those systems configured with a KIV-7 encryption device, access to the SIPRNET and other secure voice and data networks is possible. However, importantly, the disclosed deployable secure communication system also provides an access point

for a direct link to a local enterprise network providing IP encapsulated information for transmission over a network such as the Internet. In this way, bulk encrypted data may be routed using an available link (e.g., a wired Ethernet port in a hotel room, high speed cable, etc.) Thus, secure data communications and/or voice-over-IP communications over the Internet are possible.

The disclosed deployable communication system provides a single user, or multiple users, remote secure access to a local enterprise network, and thus access to services conventionally provided only to direct connected users. Also, up to two simultaneous voice over IP calls may be established along with normal data connectivity via, e.g., a laptop computer.

Fig. 1 is a block diagram of an exemplary deployable secure communication system, in accordance with a first embodiment of the present invention.

In particular, Fig. 1 shows a deployable communications module **112** including a secure encryption module, e.g., one built according to KIV-7 requirements. On the red, non-secure side of the deployable communications module **112**, voice communications **110** and/or data communications such as from a laptop computer **111** or other digital device are provided with suitable interfaces.

For instance, the analog telephone **110** may interface with a standard 2-wire telephone loop. Alternatively, the telephone may be a digital telephone and be provided with an ISDN type digital subscriber link to the deployable communications module **112**. The laptop computer may communicate with the deployable communications module **112** using a standard Ethernet 10baseT or 100baseT type network link.

On the black, or secure side, the disclosed deployable system includes an Inmarsat M4 terminal **114** providing a direct connection to an enterprise network via a satellite. The M4 Satellite

terminal is, e.g., a Nera WorldCommunicator portable Inmarsat M4 satellite terminal, which is a portable Inmarsat M4 satellite terminal capable of providing 64kbps ISDN connectivity to remote users. Additional features include a 3-panel antenna with RF transceiver; a wireless DECT 2.4Ghz Handset; and a modem unit and battery pack.

Importantly, the present invention also provides an Ethernet direct connection to a local enterprise network, e.g., a hotel Ethernet network having direct access to the Internet, high speed cable, etc. Thus, when the deployable communication system is in the convenience of modern accommodations, such as in a hotel or other public place that provides an Ethernet link to the Internet, such services may be utilized without the need to set up the direct connection using the Inmarsat M4 terminal **114**.

It is important to understand that this direct connection to the Internet is on the black side of the deployable communication system, thus bulk encrypted data (i.e., secure data) may be conveniently routed along the public Internet **101** to a desired destination. This saves bandwidth on the relevant satellite, and also battery power necessary to drive the satellite transceiver. It also simply provides secure communications while in a hotel room or similar public place, near a cable modem, etc.

Fig. 2 is a more detailed block diagram of the exemplary deployable secure communication system shown in Fig. 1.

In particular, as shown in Fig. 2, the deployable communications module **112** includes a black (encrypted, or secure) portion and a red (non-encrypted, or unsecure) portion.

The red portion includes a router **202**, e.g., a Cisco 1751-V voice enabled modular access router. This router 202 includes one fast Ethernet (10/100BaseTX) port; Interface cards support either WIC or VIC modules; and it supports VoIP, VoFR, and VoATM connections.

The red portion also includes a suitable power supply such as the +5V, +12V and –12V power supply **212** shown in Fig. 2. The red components are shielded in a suitable RFI/EMI shielding preferably providing –40dB to –60dB of isolation. The compartment in which the red components sit may also be coated with a suitable RFI/EMI isolating coating.

The black portion includes a KIV-7 device **200** such as the KIV-7HSB shown in Fig. 2. The disclosed KIV-7HSB is a Mykotronx KIV-7 module is a standard compact, economical, high performance, and user-friendly COMSEC device, designed to meet users' needs for secure data communication links. Features of this unit include Commercial Off-the-shelf (COTS) Type I data encryption; KG-84/-84A/-84C interoperability; User-friendly menu-based operator interface; and Standard D-type rear-panel interface connectors.

An IP tube **204** such as that commercially available from Engage Communications encapsulates encrypted data, and passes it either to an Ethernet port which may be wired directly to an Ethernet network having access to the Internet **101**, or to a black-side router **206** (e.g., commercially available from CISCO). The router **206** includes an ISDN port (ISDN/BRI/ST) to link to the Inmarsat M4 terminal **114**.

The KIV-7 preferably uses a serial RS-530 connection both on its red side to the red side router **202**, as well as on the black side to connect to the IP tube **204**. The red side router **202** is suitably configured for operation with the KIV-7 encryption device **200**.

The red side router **202** is configured to allow for transparent, automated operation for the user. All off-network traffic is routed via the serial port to the KIV-7HSB for bulk encryption. In addition, the voice ports are configured so that dialing a "9" (or any other string desired by the user) will result in off-network traffic and be routed to the distant end gateway.

The IP tube **204** has firmware modified from that otherwise commercially available to allow acceptance of encrypted data. The firmware was modified so that the IP Tube clock could be tuned to match the output of the KIV-7HSB. In addition, the firmware was also modified to allow for a dial-on-demand feature so the unit would be in an idle state until interesting traffic were presented.

The laptop computer **111a** depicts in solid line a one-to-one connection into the red side router **202**. In a dotted line depiction, multiple computing devices **111a-111b** may be networked over a conventional Ethernet network **111c**, with the red side router **202** being a member of that Ethernet network **111c**.

Any computing device capable of an Ethernet connection may be implemented. In the disclosed embodiment, the laptop computers that were implemented were Panasonic Toughbooks™. Those laptop computers are ruggedized in that it is shock, dust, vibration and water resistant, making it a good choice for a deployable communication system. Additional features include design to MIL-STD-810F test procedures; and password security (Supervisor, User), "Access Key".

The deployable communication system communicates over the Internet (considered black with respect to the bulk encrypted data passed through the Ethernet port of the IP tube **204**) with a suitable IP gateway (not shown). As long as both sides know the IP address of the other, and the IP tube **204** is properly configured, communications will be enabled.

The IP Tube is configured so as to seek a specific distant end device and establish a dedicated tunnel. The internal side of the IP Tube is configured to seek a specific (distant end) IP address. The distant end device is configured to seek the opposite. Once located the two devices communicate and establish the tunnel.

Both the red side router **202** and the black side router **206** are configured to maintain QOS. The link fragmentation and packet interleaving are preferably implemented to assure voice quality. PPP multilinking may be utilized to maximize performance.

The routing information is not passed through the KIV-7HSB **200**. The black side router **206** provides the routing of the WAN link. The red side router **202** provides the routing information for the network traffic and is contained in the encrypted payload. This information is passed from red side router **202** to red side router.

The disclosed deployable communication system provides up to two simultaneous voice-over-IP calls along with normal data connectivity. Connectivity between the remote system and the enterprise network is provided by the Inmarsat M4 terminal, through connection to a terrestrial ISDN circuit, or by connection to a network or the Internet. Transmissions between the deployed system and enterprise network are encrypted and fully secure up through the Top Secret level through the use of a KIV-7 bulk encryption device.

Importantly, the deployable communication system allows for routing of bulk encrypted data, a feature not available in any other deployable communication system employing a KIV-7 encryption device.

In the disclosed embodiment, commercial off the shelf (COTS) equipment is integrated at the board level into an outer case made of high quality plastics. The COTS (i.e., commercially available) equipment includes the Cisco 1751V router **202**, the Cisco 801 router **206**, the Engage Communications RS-530 IP Tube **204**, the KIV-7HSB encryption unit 200, the tri-volt power supply **212**, the DC power supply **210**, and a DC/AC inverter **208**.

Individual components are preferably integrated in such a manner so as to provide separation between encrypted and non-encrypted data, and to ensure protection of the components. Additionally,

the specific integration and configuration of the system allows for operation by simply deploying the M4 terminal and applying power. Ideally, the deployable communication system **112** can be powered by universal AC input or by 12 VDC from a vehicle cigarette lighter.

Data entering the deployable communication system **112** and destined for the enterprise network is routed by the red side router **202** and passed to the encryption unit **200** for encryption. Once encrypted, the data is then passed to the RS-530 IP tube **204**, where it is encapsulated into IP packets and passed to the black side Cisco 801 Ethernet to ISDN router **206**.

This data is then passed out of the ISDN port of the black side router **206**, and on to the direct connection to the Inmarsat M4 Terminal **114**, where it is transmitted to the enterprise network.

The deployable communication system **112** accomplishes two specific functions during transmission.

Firstly, an IPSEC tunnel is established between the black side router **206** and a gateway router at the receiving fixed enterprise. This provides privacy for the overall link. Moreover, and importantly, it presents a commercial/civilian appearance to the transmitted encrypted signal.

Secondly, another tunnel is established between the deployed RS-530 tube **204** and another IP tube at the fixed enterprise network. With this second tunnel established, the bulk encrypted data from the KIV-7 type encryption unit **200**, which is normally non-routable, is encapsulated in IP packets and routed to the distant end network.

Data encrypted by the KIV-7HSB encryption module **200** normally requires a dedicated, point-to-point circuit for communications to be successful. This is significant for two reasons.

First, through the use of the disclosed deployable communication system bulk encrypted data can be routed, thus making

use of generic IP or network connections. Moreover, while the deployable communication system would normally be operated with a direct, one to one connection via the Inmarsat M4 Terminal **114**, the process of encapsulating the bulk encrypted data into IP packets, and thus routing of the bulk encrypted data, allows for connecting the system into any network—or directly into the Internet via the Ethernet port made available at the output of the IP tube **204**.

Second, the unique signature of the government used Type 1 encryption is masked by the two separate tunnels and appears as normal commercially encrypted data, thus providing a level of cover to individual operators.

The deployable communications system preferably includes grounding incorporated into grounded AC Power, and is contained in a single deployable case. The disclosed deployable communication system measured about 17"x12"x5" and weighed about 40 pounds, though other small measurements and light weight systems are within the scope of the present invention.

Preferably, expansion capabilities may be implemented to support additional users. Moreover, multiple connectivity may be provided by including flexible connection methods and speeds for voice, video and data services, including: a VSAT terminal, an ISDN terminal, an Inmarsat terminal, a conventional dial-up modem, and operate in either a secure or non-secure communications mode.

A single case deployable communications system in accordance with the principles of the present invention has particular application with the US military, federal, local and state agencies, disaster recovery agencies, public safety associations, news channels, and commercial enterprises, to name a few.

The disclosed deployable communication system preferably allows for operation "out of the box", meaning the only component

requiring removal is the M4 terminal. Moreover, the deployable communication system is preferably of a size and weight so as to be capable of transport on commercial aircraft as checked baggage.

Figs. 3 to 8 depict another embodiment of a deployable secure communication system in accordance with another aspect of the present invention.

In particular, Fig. 3 shows a graphic depiction of another exemplary deployable communication system in communication with a gateway network, in accordance with another aspect of the present invention.

As shown in Fig. 3, laptops **302** and telephones 304 are shown being routed by a router, encrypted by a KIV-7 device, and routed to an Inmarsat M4 terminal that communicates through a satellite.

Fig. 4 shows an exemplary network server module, in accordance with the principles of the present invention.

Fig. 5 shows an exemplary network WAN module, in accordance with the principles of the present invention.

Fig. 6 shows an exemplary network encryption module based on a KIV-21, in accordance with the principles of the present invention.

In particular, Fig. 6 shows a Network Encryption D-LAN MAIN module. The NEM provides NSA Type 1 encryption for network operations. With this module all traffic entering or leaving the network is fully encrypted up to a level of TS. As configured the module consists of a Cisco 3640 router with five (5) Ethernet ports and two (2) ISDN PRI ports, and the new KIV-21 IP encryption device manufactured by VIASAT. One advantage to using the KIV-21 as opposed to older devices is the ability to establish a point-to-multipoint, fully meshed network. Unlike legacy devices such as the KIV-7, KIV-19 and KG type units that could only establish a point-to-point connection with a matched device, each KIV-21

in the network can communicate directly with any other KIV-21 containing a compatible key. This allows significant improvement in communications while limiting the size and weight of the total deployable package. Although configured with the KIV-21 for this requirement, any existing encryption device can be integrated into the system as user requirements dictate. In addition, commercially available, non Type 1 devices/software can be integrated into the LPDCS for commercial/non US Government applications. The module is integrated into a custom roll-around case measuring 21"W x 15"L x 9"D and weighs about 55 lbs.

Fig. 7 shows a universal power module, in accordance with the principles of the present invention.

In particular, Fig. 7 shows a universal power module. It is preferred that each of the disclosed systems operate from universal AC power sources, have built-in battery backup supporting all system components for a minimum of 15 minutes, and also have the ability to be supplied with an external DC power source. To satisfy this requirement we evaluated numerous commercially available UPS systems, but found none that met size, weight and operational parameters. The UPSI 1000 and 1400 series UPS provided the universal AC input requirement, but did not allow for external DC input and exceeded the 70 lb weight restriction. Our next alternative was to evaluate designing a smaller AC source and UPS into each of the individual module cases, but again this proved to be ineffective because of weight and size issues. Our final solution was to design an independent power module capable of powering the entire system. UPM was assembled using commercial-off-the-shelf equipment and consists of one (1) universal front end, one (1) DC to AC power inverter, two (2) 12 volt batteries and a main power switch.

Fig. 8 shows a low profile deployable secure communication system integrating a network server module, a network WAN module, an

encryption module, and a universal power module, in accordance with the principles of yet another aspect of the present invention.

A universal front end accepts between 86-240VAC and provides 24 volts DC to the on-board batteries and the DC/AC inverter. The inverter conditions the power and provides a stable 110 VAC output for the network components. In the event of commercial power loss, the on-board batteries are sufficient to support operations for the required minimum of 15 minutes and have been tested to operate in excess of 45 minutes. Operation of all system components in a hot standby mode has been demonstrated in excess of two hours. In the event the internal batteries are depleted prior to commercial power restoration, two external 12 volt car batteries can be jumper together and connected into the module for continued operation. This module is integrated into a custom roll-around case measuring 15"W x 24"L x9"D and weighs about 72 lbs including batteries.

While the invention has been described with reference to the exemplary embodiments thereof, those skilled in the art will be able to make various modifications to the described embodiments of the invention without departing from the true spirit and scope of the invention.